

CLAIMS

What is claimed is:

- 1 1. A method for controlling and tracking access to a message that is communicated
2 from a first node to a second node in a network, the method comprising the
3 computer-implemented steps of:
4 receiving a request from the first node for a message identifier that uniquely
5 identifies the message and a key that may be used to encode the message;
6 generating, in response to the request, both the message identifier and the key;
7 providing both the message identifier and the key to the first node to allow the
8 message to be encoded with the key to generate an encoded message;
9 receiving a request from the second node for the key;
10 generating algorithm identification data that indicates an algorithm to be used to
11 decode the encoded message;
12 providing the algorithm identification data to the second node;
13 providing the key and the identification data to the second node to allow the
14 encoded message to be decoded and the message to be retrieved using the
15 key; and
16 deleting the key based upon specified key policy criteria to prevent copies of the
17 encoded message from being decoded.
- 1 2. The method as recited in Claim 1, further comprising:
2 receiving a second request from the first node for a second message identifier that
3 uniquely identifies a second message and a second key that may be used to
4 encode the second message;
5 generating, in response to the second request, both the second message identifier
6 and the second key;

7 providing both the second message identifier and the second key to the first node
8 to allow the second message to be encoded with the second key to generate
9 a second encoded message;
10 receiving a second request from the second node for the second key;
11 generating second algorithm identification data that indicates a second algorithm
12 to be used to decode the second encoded message;
13 providing the second algorithm identification data to the second node;
14 providing the second key and the second identification data to the second node to
15 allow the second encoded message to be decoded and the second message
16 to be retrieved using the second key; and
17 deleting the second key based upon the specified key policy criteria to prevent
18 copies of the second encoded message from being decoded.

1 3. The method as recited in Claim 1, wherein the decoding identification data
2 further indicates a location wherein the algorithm can be found.

1 4. The method as recited in Claim 1, wherein the algorithm identification data is
2 generated at the first node.

1 5. The method as recited in Claim 1, wherein the algorithm identification data is
2 stored at a key repository.

1 6. A computer-readable medium carrying one or more sequences of one or more
2 instructions for controlling and tracking access to a message that is
3 communicated from a first node to a second node in a network, the one or more
4 sequences of one or more instructions including instructions which, when
5 executed by one or more processors, cause the one or more processors to perform
6 the steps of:
7 receiving a request from the first node for a message identifier that uniquely
8 identifies the message and a key that may be used to encode the message;
9 generating, in response to the request, both the message identifier and the key;

10 providing both the message identifier and the key to the first node to allow the
11 message to be encoded with the key to generate an encoded message;
12 receiving a request from the second node for the key;
13 generating algorithm identification data that indicates an algorithm to be used to
14 decode the encoded message;
15 providing the algorithm identification data to the second node;
16 providing the key and the identification data to the second node to allow the
17 encoded message to be decoded and the message to be retrieved using the
18 key; and
19 deleting the key based upon specified key policy criteria to prevent copies of the
20 encoded message from being decoded.

1 7. The computer-readable medium as recited in Claim 6, wherein the one or more
2 sequences of one or more instructions include one or more additional sequences
3 of one or more additional instructions which, when executed by the one or more
4 processors, cause the one or more processors to perform the steps of:
5 receiving a second request from the first node for a second message identifier that
6 uniquely identifies a second message and a second key that may be used to
7 encode the second message;
8 generating, in response to the second request, both the second message identifier
9 and the second key;
10 providing both the second message identifier and the second key to the first node
11 to allow the second message to be encoded with the second key to generate
12 a second encoded message;
13 receiving a second request from the second node for the second key;
14 generating second algorithm identification data that indicates a second algorithm
15 to be used to decode the second encoded message;
16 providing the second algorithm identification data to the second node;

17 providing the second key and the second identification data to the second node to
18 allow the second encoded message to be decoded and the second message
19 to be retrieved using the second key; and
20 deleting the second key based upon the specified key policy criteria to prevent
21 copies of the second encoded message from being decoded.

1 8. The computer-readable medium as recited in Claim 6, wherein the decoding
2 identification data further indicates a location wherein the algorithm can be
3 found.

1 9. The computer-readable medium as recited in Claim 6, wherein the algorithm
2 identification data is generated at the first node.

1 10. The computer-readable medium as recited in Claim 6, wherein the algorithm
2 identification data is stored at a key repository.

1 11. A computer system for controlling and tracking access to a message that is
2 communicated from a first node to a second node in a network comprising:
3 one or more processors; and
4 a memory communicatively coupled to the one or more processors and carrying
5 one or more sequences of one or more instructions which, when executed
6 by the one or more processors, cause the one or more processors to
7 perform the steps of:
8 receiving a second request from the first node for a second message
9 identifier that uniquely identifies a second message and a second
10 key that may be used to encode the second message;
11 generating, in response to the second request, both the second message
12 identifier and the second key;
13 providing both the second message identifier and the second key to the
14 first node to allow the second message to be encoded with the
15 second key to generate a second encoded message;

16 receiving a second request from the second node for the second key;
17 generating second algorithm identification data that indicates a second
18 algorithm to be used to decode the second encoded message;
19 providing the second algorithm identification data to the second node;
20 providing the second key and the second identification data to the second
21 node to allow the second encoded message to be decoded and the
22 second message to be retrieved using the second key; and
23 deleting the second key based upon the specified key policy criteria to
24 prevent copies of the second encoded message from being decoded.

1 12. The computer system as recited in Claim 11, wherein the memory further includes
2 one or more additional sequences of one or more instructions which, when
3 executed by the one or more processors, cause the one or more processors to
4 perform the steps of:
5 receiving a second request from the first node for a second message identifier that
6 uniquely identifies a second message and a second key that may be used to
7 encode the second message;
8 generating, in response to the second request, both the second message identifier
9 and the second key;
10 providing both the second message identifier and the second key to the first node
11 to allow the second message to be encoded with the second key to generate
12 a second encoded message;
13 receiving a second request from the second node for the second key;
14 generating second algorithm identification data that indicates a second algorithm
15 to be used to decode the second encoded message;
16 providing the second algorithm identification data to the second node;
17 providing the second key and the second identification data to the second node to
18 allow the second encoded message to be decoded and the second message
19 to be retrieved using the second key; and
20 deleting the second key based upon the specified key policy criteria to prevent
21 copies of the second encoded message from being decoded.

- 1 13. The computer system as recited in Claim 11, wherein the decoding identification
2 data further indicates a location wherein the algorithm can be found.
- 1 14. The computer system as recited in Claim 11, wherein the algorithm identification
2 data is generated at the first node.
- 1 15. The computer system as recited in Claim 11, wherein the algorithm identification
2 data is stored at a key repository.
- 1 16. A method for controlling access to a message that is communicated from a first
2 node to a second node in a network, the method comprising the computer-
3 implemented steps of:
4 generating, at the first node, an encoded message by encoding the message with a
5 key;
6 generating, at the first node, a set of one or more instructions that contain the
7 encoded message and instructions for decoding the encoded message
8 using the key; and
9 providing the set of one or more instructions to the second node;
10 wherein, processing the set of one or more instructions at the second node causes
11 the message to be recovered from the encoded message contained in the
12 set of one or more instructions by:
13 retrieving the key, and
14 decoding the encoded message using the key.
- 1 17. The method as recited in Claim 16, further comprising deleting the retrieved key.
- 1 18. The method as recited in Claim 16, wherein the set of one or more instructions
2 comprises a set of Javascript instructions.

- 1 19. The method as recited in Claim 16, wherein the set of one or more instructions
2 comprises a set of Java applet instructions.
- 1 20. The method as recited in Claim 16, wherein the set of one or more instructions
2 includes address data that indicates a location from which the key may be
3 retrieved.
- 1 21. A computer-readable medium for controlling access to a message that is
2 communicated from a first node to a second node in a network, the computer-
3 readable medium carrying one or more sequences of one or more instructions
4 which, when executed by one or more processors, cause the one or more
5 processors to perform the steps of:
6 generating, at the first node, an encoded message by encoding the message with a
7 key;
8 generating, at the first node, a set of one or more instructions that contain the
9 encoded message and instructions for decoding the encoded message
10 using the key; and
11 providing the set of one or more instructions to the second node;
12 wherein, processing the set of one or more instructions at the second node causes
13 the message to be recovered from the encoded message contained in the
14 set of one or more instructions by:
15 retrieving the key, and
16 decoding the encoded message using the key to recover the
17 original message.
- 1 22. The computer-readable medium as recited in Claim 21, further carrying one or
2 more additional sequences of one or instructions which, when executed by the
3 one or more processors, causes the one or more processors to perform the
4 additional step of deleting the retrieved key.

1 23. The computer-readable medium as recited in Claim 21, wherein the set of one or
2 more instructions comprises a set of Javascript instructions.

1 24. The computer-readable medium as recited in Claim 21, wherein the set of one or
2 more instructions comprises a set of Java applet instructions.

1 25. The computer-readable medium as recited in Claim 21, wherein the set of one or
2 more instructions include address data that indicates a location from which the
3 key may be retrieved.

1 26. A computer system comprising:
2 one or more processors; and
3 a memory communicatively coupled to the one or more processors and carrying
4 one or more sequences of one or more instructions which, when executed
5 by the one or more processors, cause the one or more processors to
6 perform the steps of:
7 generating, at the first node, an encoded message by encoding the message with a
8 key;
9 generating, at the first node, a set of one or more instructions that contain the
10 encoded message and instructions for decoding the encoded message
11 using the key; and
12 providing the set of one or more instructions to the second node;
13 wherein, processing the set of one or more instructions at the second node causes
14 the message to be recovered from the encoded message contained in the
15 set of one or more instructions by:
16 retrieving the key, and
17 decoding the encoded message using the key to recover the
18 original message.

1 27. The computer system as recited in Claim 26, wherein the memory further carries
2 one or more additional sequences of one or instructions which, when executed by

3 the one or more processors, causes the one or more processors to perform the
4 additional step of deleting the retrieved key.

1 28. The computer system as recited in Claim 26, wherein the set of one or more
2 instructions comprises a set of Javascript instructions.

1 29. The computer system as recited in Claim 26, wherein the set of one or more
2 instructions comprises a set of Java applet instructions.

1 30. The computer system as recited in Claim 26, wherein the set of one or more
2 instructions include address data that indicates a location from which the key may
3 be retrieved.

1 31. A method for controlling access to a message that is communicated from a first
2 node to a second node in a network, the method comprising the computer-
3 implemented steps of:
4 generating, at the first node, an encoded message by encoding the message with a
5 key;
6 generating, at the first node, a set of one or more instructions that contain the
7 encoded message and instructions for transferring to a third node the
8 encoded message and instructions for retrieving the key ;
9 providing the set of one or more instructions to the second node;
10 wherein, processing the set of one or more instructions at the second node causes
11 the encoded message and the instructions for retrieving the key to be
12 transferred to the third node; and
13 wherein, the receiving, at the third node, of the encoded message and the
14 instructions for retrieving the key causes:
15 the message to be recovered from the encoded message by
16 retrieving the key, and
17 decoding the encoded message using the key, and

18 the recovered message to be provided from the third node to the second
19 node.

1 32. The method as recited in Claim 31, wherein the receiving, at the third node, of
2 the encoded message and the instructions for retrieving the key, further causes the
3 key to be deleted from the third node after the encoded message is decoded.

1 33. The method as recited in Claim 31, wherein the set of one or more instructions
2 that contain the encoded message and instructions for transferring to a third node
3 the encoded message and instructions for retrieving the key comprises an HTML
4 document.

1 34. The method as recited in Claim 33, wherein the HTML document comprises an
2 HTML form with fields containing the encoded message and key address data, a
3 submit button to submit the form to the third node, and JavaScript to
4 automatically submit the form to the third node.

1 35. The method as recited in Claim 33, wherein the HTML document comprises a set
2 of associated URLs embedded in multiple , <ilayer>, <applet>, or <iframe>
3 elements, wherein each URL contains fragments of the encoded message and key
4 address data as URL query parameters, and wherein each URL specifies the
5 location of the third node.

1 36. The method as recited in Claim 35, wherein the URL query parameters also
2 contain control information, which specifies the order and number of message
3 fragments, and enables the third node to reconstruct the complete message.

1 37. A computer-readable medium for controlling access to a message that is
2 communicated from a first node to a second node in a network, the computer-
3 readable medium carrying one or more sequences of one or more instructions

4 which, when executed by one or more processors, cause the one or more
5 processors to perform the steps of:
6 generating, at the first node, an encoded message by encoding the message with a
7 key;
8 generating, at the first node, a set of one or more instructions that contain the
9 encoded message and instructions for transferring to a third node the
10 encoded message and instructions for retrieving the key ;
11 providing the set of one or more instructions to the second node;
12 wherein, processing the set of one or more instructions at the second node causes
13 the encoded message and the instructions for retrieving the key to be
14 transferred to the third node; and
15 wherein, the receiving, at the third node, of the encoded message and the
16 instructions for retrieving the key causes:
17 the message to be recovered from the encoded message by
18 retrieving the key, and
19 decoding the encoded message using the key, and
20 the recovered message to be provided from the third node to the second
21 node.

1 38. The computer-readable medium as recited in Claim 37, wherein the receiving, at
2 the third node, of the encoded message and the instructions for retrieving the key,
3 further causes the key to be deleted from the third node after the encoded
4 message is decoded.

1 39. The computer-readable medium as recited in Claim 37, wherein the set of one or
2 more instructions that contain the encoded message and instructions for
3 transferring to a third node the encoded message and instructions for retrieving
4 the key comprises an HTML document.

1 40. The computer-readable medium as recited in Claim 39, wherein the HTML
2 document comprises an HTML form with fields containing the encoded message

3 and key address data, a submit button to submit the form to the third node, and
4 JavaScript to automatically submit the form to the third node.

1 41. The computer-readable medium as recited in Claim 39, wherein the HTML
2 document comprises a set of associated URLs embedded in multiple ,
3 <ilayer>, <applet>, or <iframe> elements, wherein each URL contains fragments
4 of the encoded message and key address data as URL query parameters, and
5 wherein each URL specifies the location of the third node.

1 42. The computer-readable medium as recited in Claim 41, wherein the URL query
2 parameters also contain control information, which specifies the order and number
3 of message fragments, and enables the third node to reconstruct the complete
4 message.

1 43. A computer system for controlling access to a message that is communicated
2 from a first node to a second node in a network, the computer system comprising:
3 one or more processors; and
4 a memory communicatively coupled to the one or more processors and carrying
5 one or more sequences of one or more instructions which, when executed
6 by the one or more processors, causes the one or more processors to
7 perform the steps of:
8 generating, at the first node, an encoded message by encoding the
9 message with a key;
10 generating, at the first node, a set of one or more instructions that contain
11 the encoded message and instructions for transferring to a third
12 node the encoded message and instructions for retrieving the key;
13 providing the set of one or more instructions to the second node;
14 wherein, processing the set of one or more instructions at the second node
15 causes the encoded message and the instructions for retrieving the
16 key to be transferred to the third node; and

17 wherein, the receiving, at the third node, of the encoded message and the
18 instructions for retrieving the key causes:
19 the message to be recovered from the encoded message by
20 retrieving the key, and
21 decoding the encoded message using the key, and
22 the recovered message to be provided from the third node to the
23 second node.

1 44. The computer system as recited in Claim 43, wherein the receiving, at the third
2 node, of the encoded message and the instructions for retrieving the key, further
3 causes the key to be deleted from the third node after they encoded message is
4 decoded.

1 45. The computer system as recited in Claim 43, wherein the set of one or more
2 instructions that contain the encoded message and instructions for transferring to
3 a third node the encoded message and instructions for retrieving the key
4 comprises an HTML document.

1 46. The computer system as recited in Claim 45, wherein the HTML document
2 comprises an HTML form with fields containing the encoded message and key
3 address data, a submit button to submit the form to the third node, and JavaScript
4 to automatically submit the form to the third node.

1 47. The computer system as recited in Claim 45, wherein the HTML document
2 comprises a set of associated URLs embedded in multiple , <ilayer>,
3 <applet>, or <iframe> elements, wherein each URL contains fragments of the
4 encoded message and key address data as URL query parameters, and wherein
5 each URL specifies the location of the third node.

1 48. The computer system as recited in Claim 47, wherein the URL query parameters
2 also contain control information, which specifies the order and number of message
3 fragments, and enables the third node to reconstruct the complete message.

1 49. A method for exchanging data between nodes in a network, the method
2 comprising the computer-implemented steps of:
3 embedding, in one or more associated URLs, data and control information; and
4 providing the set of one or more associated URLs from a source node to a
5 destination node; and
6 wherein the data and control information may be extracted from the set of one or
7 more associated URLs at the destination node.

1 50. The method as recited in Claim 49, wherein the set of one or more associated
2 URLs is provided from the source node to the destination node using the HTTP
3 protocol.

1 51. The method as recited in Claim 50, wherein the set of one or more associated
2 URLs is contained within an HTML document.

1 52. The method as recited in Claim 51, wherein each URL from the set of one or more
2 associated URLs, contained within the HTML document, is embedded in an
3 , <ilayer>, <applet>, or <iframe> element, contains fragments of the data as
4 URL query parameters, and specifies a location of the destination node.

1 53. The method as recited in Claim 52, wherein the URL query parameters also
2 contain control information, which specifies an order and number of data
3 fragments to enable the data to be reconstructed at the destination node.

1 54. The method as recited in Claim 53, wherein:

2 the HTML document is embedded in a registration email received at the source
3 node, the data embedded in the one or more associated URLs includes
4 registration and user information, and
5 the method further comprises the computer-implemented steps of:
6 providing the data to the destination node when the registration email is
7 read;
8 generating an authentication cookie on the source node in response to
9 receiving the registration and user information;
10 using the authentication cookie to authenticate a user at the source node
11 when the source node makes subsequent client requests to the
12 destination node.

1 55. A computer-readable medium for exchanging data between nodes in a network,
2 the computer-readable medium carrying one or more sequences of one or more
3 instructions which, when executed by one or more processors, cause the one or
4 more processors to perform the steps of:
5 embedding, in one or more associated URLs, data and control information; and
6 providing the set of one or more associated URLs from a source node to a
7 destination node;
8 wherein the data and control information may be extracted from the set of one or
9 more associated URLs at the destination node.

1 56. The computer-readable medium as recited in Claim 55, wherein the set of one or
2 more associated URLs is provided from the source node to the destination node
3 using the HTTP protocol.

1 57. The computer-readable medium as recited in Claim 56, wherein the set of one or
2 more associated URLs is contained within an HTML document.

1 58. The computer-readable medium as recited in Claim 57, wherein each URL from
2 the set of one or more associated URLs, contained within the HTML document, is
3 embedded in an , <ilayer>, <applet>, or <iframe> element, contains
4 fragments of the data as URL query parameters, and specifies a location of the
5 destination node.

1 59. The computer-readable medium as recited in Claim 58, wherein the URL query
2 parameters also contain control information, which specifies an order and number
3 of data fragments to enable the data to be reconstructed at the destination node.

1 60. The computer-readable medium as recited in Claim 59, wherein:
2 the HTML document is embedded in a registration email received at the source
3 node, the data embedded in the one or more associated URLs includes
4 registration and user information, and
5 the computer-readable medium further comprises one or more additional
6 sequences of one or more instructions which, when executed by the one or
7 more processors, causes the one or more processors to perform the
8 computer-implemented steps of:
9 providing the data to the destination node when the registration email is
10 read;
11 generating an authentication cookie on the source node in response to
12 receiving the registration and user information;
13 using the authentication cookie to authenticate a user at the source node
14 when the source node makes subsequent client requests to the
15 destination node.

1 61. A computer system comprising:
2 one or more processors; and
3 a memory communicatively coupled to the one or more processors and carrying
4 one or more sequences of one or more instructions which, when executed

5 by the one or more processors, cause the one or more processors to
6 perform the steps of:
7 embedding, in one or more associated URLs, data and control information;
8 and
9 providing the set of one or more associated URLs from a source node to a
10 destination node;
11 wherein the data and control information may be extracted from the set of
12 one or more associated URLs at the destination node.
13

1 62. The computer system as recited in Claim 61, wherein the set of one or more
2 associated URLs is provided from the source node to the destination node using
3 the HTTP protocol.

1 63. The computer system as recited in Claim 62, wherein the set of one or more
2 associated URLs is contained within an HTML document.

1 64. The computer system as recited in Claim 63, wherein each URL from the set of
2 one or more associated URLs, contained within the HTML document, is
3 embedded in an , <ilayer>, <applet>, or <iframe> element, contains
4 fragments of the data as URL query parameters, and specifies a location of the
5 destination node.

1 65. The computer system as recited in Claim 64, wherein the URL query parameters
2 also contain control information, which specifies an order and number of data
3 fragments to enable the data to be reconstructed at the destination node.

1 66. The computer system as recited in Claim 65, wherein:
2 the HTML document is embedded in a registration email received at the source
3 node, the data embedded in the one or more associated URLs includes
4 registration and user information, and

5 the memory further comprises one or more additional sequences of one or more
6 instructions which, when executed by the one or more processors, causes
7 the one or more processors to perform the computer-implemented steps of:
8 providing the data to the destination node when the registration email is
9 read;
10 generating an authentication cookie on the source node in response to
11 receiving the registration and user information;
12 using the authentication cookie to authenticate a user at the source node
13 when the source node makes subsequent client requests to the
14 destination node.